



FortiToken Mobile 2.2

User Guide for iOS



FortiToken Mobile 2.2 User Guide for iOS

November 22, 2013

33-22-211628-20131122

Copyright © 2013 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

FortiToken Mobile for iOS.....	4
Introduction.....	4
Overview	4
Supported Versions and Devices.....	4
Apple iOS	4
Installing the FTM Application	4
Downloading FTM for Apple iOS	4
Token Activation	4
FortiToken Activation Email/SMS Message.....	4
Activating your Token	5
Scan Barcode	7
Manual Activation.....	7
Third-Party Token Activation	9
Using the FortiToken Mobile Application.....	10
Generating OTPs.....	10
Copying and Pasting OTPs to/from Clipboard	10
Application Timeout	10
FTM Features	10
Managing Tokens.....	10
Adding Tokens	11
Deleting Tokens	11
Edit Token Name.....	11
Change Default Token	11
Alerts and Troubleshooting.....	11
Activation Issues	11
Synchronization Issues	11

FortiToken Mobile for iOS

Introduction

The FortiToken Mobile (FTM) is an application that allows you to generate One Time Password (OTP) values on your mobile device for use in two-factor authentication. Once your token is activated, you will not need any network access to generate OTPs on your device.

Overview

First you will install the application. Once the app is installed on your mobile device, you will need to activate a token. After the token is activated, you can immediately generate OTPs on your device.

Supported Versions and Devices

The application can be installed on iPhones, iPads and iPod Touch devices. No cellular network is required; if you don't have cellular service, just use your WiFi access.

Apple iOS

Supported iOS Operating System versions: Apple iOS 4.x through 7.x.

Installing the FTM Application

Downloading FTM for Apple iOS

Go to the iTunes app store to download the free FortiToken Mobile application.

Click [here](#) for the FortiToken Mobile download from App Store.

After the app has been installed, make sure the device has the correct date and time. Go to *Settings > General > Date and Time* on the device and adjust as necessary.

Token Activation

The FortiToken Mobile v2 application allows you to install Fortinet tokens as well as third-party tokens, including tokens for two-step verification used by Dropbox, Google, Amazon and Microsoft.

FortiToken Activation Email/SMS Message

After your system administrator assigns your token, you will receive notification with an activation code and an activation expiration date by which you must activate your token. Depending on which option your system administrator has chosen, you will receive the activation notification either by SMS or email. If you do not activate your token by the indicated expiration date, you must contact your sysadmin so that your token can be reassigned for activation.

The activation notification looks like this:

=====

Welcome to FortiToken Mobile - One-Time-Password software token.

Please visit <http://docs.fortinet.com/ftoken.html> for instructions on how to install your FortiToken Mobile application on your device and activate your token.

You must use FortiToken Mobile version 2 to activate this token.

Your Activation Code, which you will need to enter on your device later, is

"xxxxxxxxxxxxxxxxxxxx"

A QR code image is also attached.

You must activate your token by: Sat Jun 15 01:26:14 2013 GMT+00:00, after which you will need to contact your system administrator to re-enable your activation.

=====

Activating your Token

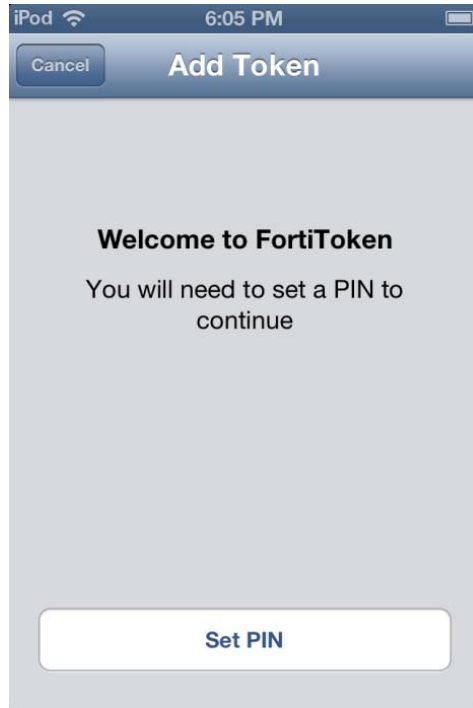
You can activate your token on FortiToken Mobile once you receive an activation code.

Before you begin, make sure your device is set to the correct time and that you have Internet access.

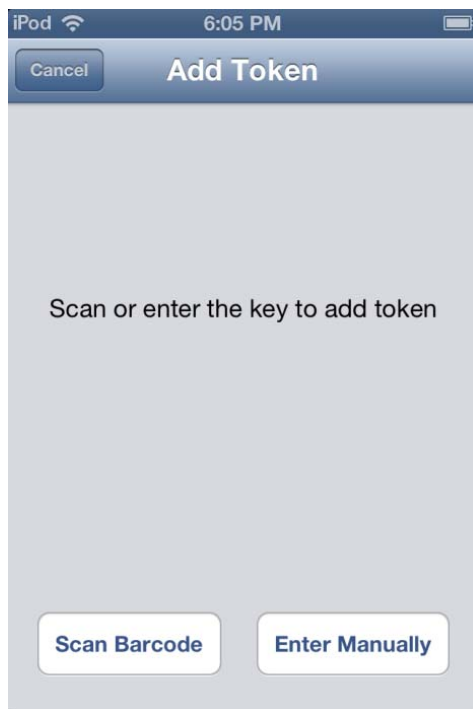
1. Start the application by touching the FortiToken Mobile icon on your device screen.



2. If there is no PIN set, you will be prompted to create a 4-digit PIN.



3. Once you have created and confirmed your PIN, you can add your tokens by using the activation code provided by your System Administrator. You can either enter the activation code manually, or you can select *Scan Barcode* if your device supports it.



Scan Barcode

If your iOS device supports QR code recognition, you can simply press *Scan Barcode* and point your device camera at the QR code attached to the activation email.



QR code images are not provided using the SMS activation message, only with the email activation message.

Manual Activation

1. Select the type of token from the list. For FortiToken, select *Fortinet*.

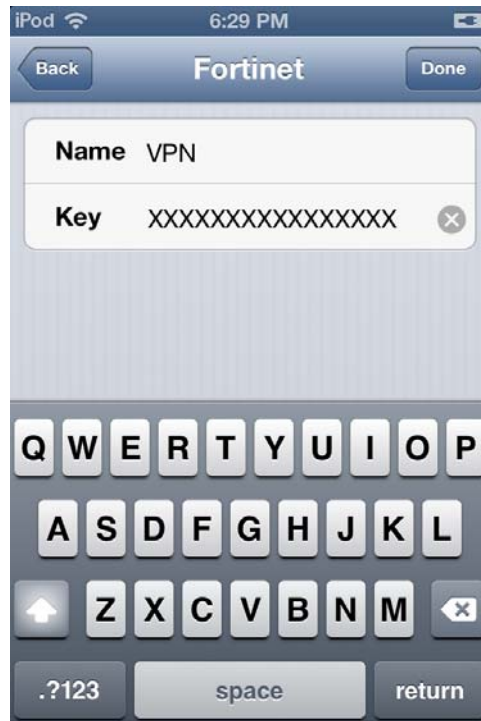


2. Enter a name for this token, and then enter the activation code exactly as it appears in your activation message, either by typing or copying and pasting.

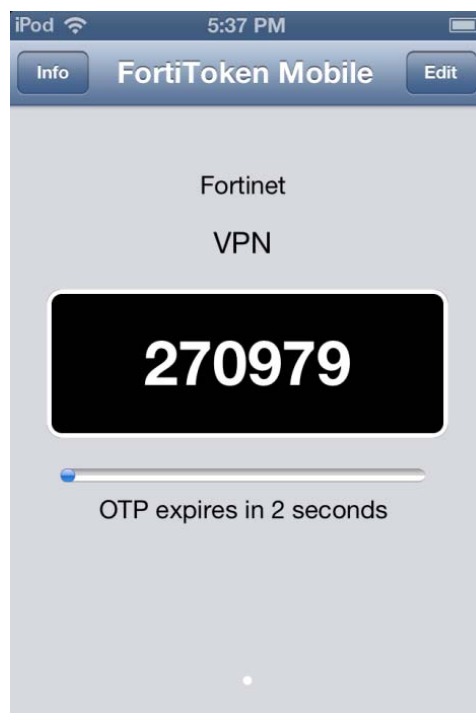


FortiToken Mobile will automatically convert lowercase to uppercase letters so there is no need to use the *Shift* key when typing.

3. After the activation code is entered, tap *Submit* or *Done*.



FTM will communicate with the Secure FTM Provisioning Server to activate your token. Once activated, you will see the OTP displayed.



Third-Party Token Activation

Many cloud and online applications offer the option to turn on two-step verification (aka two-factor authentication) for added security. FortiToken Mobile provides a simple means to install tokens from cloud service providers, including Dropbox, Google, Amazon and Microsoft. Follow the provider's instructions for turning on two-step verification and you will get to a web page displaying an activation code; with options to scan a QR code or enter the code manually if you cannot scan the bar code. Below, we show Google two-step verification as a typical example:

×


Set up Google Authenticator

Install the Google Authenticator app for iPhone.

1. On your iPhone, tap the App Store icon.
2. Search for **Google Authenticator**.
([Download from the App Store](#))
3. Tap the app, and then tap Free to download and install it.

Now open and configure Google Authenticator.

1. In Google Authenticator, tap "+", and then "Scan Barcode."
2. Use your phone's camera to scan this barcode.



Can't scan the barcode?

1. In Google Authenticator, tap +.
2. Key type: make sure "Time-based" is selected.
3. In "Account" type your full email address.
4. In "Key" type your secret key:

fp5k vg76 ptyz l3qz jo23 lhi7 o7dh vz6j

Spaces don't matter.
5. Tap Done.

Once you have scanned the barcode, enter the 6-digit verification code generated by the Authenticator app.

Code:

Verify and Save

Cancel

If you use the option to *Scan Barcode* and don't enter a token name, the token name will default to what is encoded in the QR code image for the account name. You can always edit the token name later.

FortiToken Mobile allows you to choose a specific third-party provider, but even if your provider is not listed, you can still add a token if the activation code is presented in Base32 format.

Using the FortiToken Mobile Application

Generating OTPs

Start the application and enter your PIN. The OTP is displayed on the *Home* page. The timer bar below the OTP display shows how much time is left before a new OTP value will be displayed. OTP values change every 60 seconds.

Copying and Pasting OTPs to/from Clipboard

Your OTP (aka Passcode) can be copied to the clipboard ID desired by tapping the number displayed and then tapping *copy*. This is useful in situations such as when you are using a VPN client on our mobile device and need to enter the OTP as the second factor for logging in.

Application Timeout

If you do not touch your screen for 60 seconds, the application will timeout and you will have to enter your PIN again to display the OTP.

FTM Features

You can access the *Version*, *Epoch Time*, and *Change PIN* features by tapping the *info* button on the *Home* page display.

- *Version*: This tells which version of the FTM application is installed on your device
- *Epoch Time*: This is the universal time setting that can be used to troubleshoot token synchronization issues
- *Change PIN*: Tap *Change PIN*. Enter your current PIN, then enter new PIN. Re-enter new PIN to confirm.



Managing Tokens

Touch *Edit* on the *Home* page to add/delete tokens, change token name, or change default token.

Adding Tokens

Touch + to take you to the *Add Token* screen.

Deleting Tokens

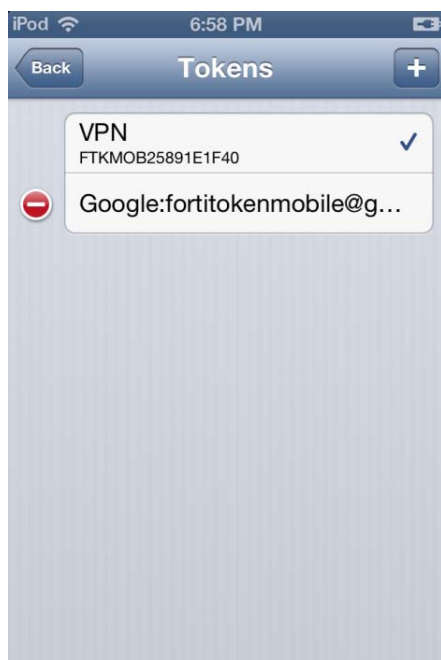
You can delete tokens directly from the *Token* screen.

Edit Token Name

Long press the token on the *Token* screen to edit the Token Name.

Change Default Token

Touch the token that you want to set as the default. The ✓ indicates the default token, which will be the token displayed on the *Home* screen.



Alerts and Troubleshooting

Activation Issues

If you receive an error message indicating that FTM timed out waiting for the server, check to make sure your device can access the Internet. If the problem persists, contact your system administrator.

If you receive an error message indicating that FTM activation failed, please check your activation code and re-enter. If the problem persists, contact your system administrator. Please supply the error code and/or error message so your administrator can correct the problem.

Synchronization Issues

If you are able to generate OTPs, but your login attempts fail, please make sure your device is set to the correct time. If the problem persists, contact your system administrator.

